UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/593,153	02/21/2008	Michael Hugh Prettejohn	P-9152-US	7291

49443 7590 07/14/2010

Pearl Cohen Zedek Latzer, LLP
1500 Broadway
12th Floor
New York, NY 10036

EXAMINER	
RAHMAN, MOHAMMAD L	
ART UNIT	PAPER NUMBER
2438	
MAIL DATE	DELIVERY MODE
07/14/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/593,153	PRETTEJOHN, MICHAEL HUGH	
	Examiner	Art Unit	
	MOHAMMAD L. RAHMAN	2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-59* is/are pending in the application.

4a) Of the above claim(s) *56-59* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-59* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 September 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *09/18/2006, 09/05/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-59 filed 09/18/2006 presented for examination. Claims 56-59 have bee canceled. Claims 1-59 are pending. At this time, claims 1-59 are rejected.

Preliminary Amendment

Preliminary amendment to the specification, filed 09/18/2006 has been acknowledged.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. 0405901.0 and 0416612.0, filed on 09/18/2006.

Information Disclosure Statement

The information disclosure statement filed 09/18/2006 and 09/05/2007 has been placed in the application file and the information referred to therein has been considered as to the merits.

Oath or Declaration

The Oath filed on 02/21/2008 complies with all the requirements set forth in MPEP 602 and therefore is accepted.

Drawings

The drawings filed on 09/18/2006 have been accepted.

Specification

The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code (see spec. page 3, 4, 13,14. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-33 are rejected under 35 U.S.C. 112, second paragraph, because

Claims 1, 14, 19, 33 element "means for storing, means for receiving, means for comparing, means for providing, means for updating, means for transmitting" is a means (or step) plus function limitation that invokes 35 U.S.C.112, sixth paragraph. However, the written description fails to disclose the corresponding structure, material, or acts for the claimed function. It is unclear whether the corresponding structure is sufficiently disclosed in the written description of the specification.

Applicant is required to:

(a) Amend the claim so that the claim limitation will no longer be a means (or step) plus function limitation under 35 U.S.C. 112, sixth paragraph; or

(b) Amend the written description of the specification such that it expressly recites what structure, material, or acts perform the claimed function without introducing any new matter (35 U.S.C. 132(a)).

If applicant is of the opinion that the written description of the specification already implicitly or inherently discloses the corresponding structure, material, or acts so that one of ordinary skill in the art would recognize what structure, material, or acts perform the claimed function, applicant is required to clarify the record by either:

(a) Amending the written description of the specification such that it expressly recites the corresponding structure, material, or acts for performing the claimed function and clearly links or

associates the structure, material, or acts to the claimed function, without introducing any new matter (35 U.S.C. 132(a)); or

(b) Stating on the record what the corresponding structure, material, or acts, which are implicitly or inherently set forth in the written description of the specification, perform the claimed function. For more information, see 37 CFR 1.75(d) and MPEP §§ 608.01(o) and 2181. Dependent claims 2-13, 15-18, 20-32 depends from claim 1, 14, and 19 do not cure the deficiencies set forth above.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-55 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-33

Claim 1,14,19 recites "A security component/A security information server….comprising means for storing....., means for receiving....., means for comparing...., means for displaying....". The recited claims do not fall within four statutory categories, do not recite any machine and can reasonably be implemented as software alone. Further, specification recites, "*features implemented in hardware may generally be implemented in software, and vice versa (see page, 8, lines 25-26*". Because of the lack of physical structure this component/server can be construed as **software per se** and is not statutory because it is not a process, machine, manufacture, or composition of

matter. Dependent claims 2-13, 15-18, 22-33 depends from claim 1, 14, and 19 do not cure the deficiencies set forth above.

Claims 34-54

With respect to claim 34, 51, the applicant's **method** steps recites storing, receiving, comparing, providing, determining, and outputting ; which fail both prong of the new Federal Circuit decision since they are not tied to and can be performed without the use of a particular apparatus, as well as not transforming any article into a different state or thing. It is also noted that the mere recitation of user terminal does not constitute statutory subject matter because the method is not implemented by machine. Dependent claims 35-50, 52-54 depends from claim 34, 51 do not cure the deficiencies set forth above. Thus claims 34-54 are non-statutory and therefore rejected.

Claims 54-55

Claims 54, 55 directed towards **program per se** as the claims recite " a computer program or computer program product" but the program is not stored in any non-transitory tangible media.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-3, 34-36, 51, 53-55 are rejected under 35 U.S.C. 102(e) as being anticipated by Reno et al. US 2005/0172229 hereinafter "Reno"

> Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Regarding claim 1, 34, Reno taught a security component (*Reno: [0005] The security application may include a plug-in to the web browser, The security application may be a tool bar, a dialog box, a popup window, a standalone application, and/or the like*) for use with an Internet browser application which displays internet resources (*Reno: [0005] The one or more resource sources may be web sites, See also [0016]*) in response to resource locators specifying the internet resources, the security component being adapted to operate alongside the Internet browser application at a user terminal / A method of providing security information to a user of an internet browser application which displays Internet resources in response to resource locators specifying the Internet resources, the browser application residing at a user terminal, the method (*Reno: [0006] a method of facilitating interaction between a user at a client device and a resource source. The client device includes a user interface through which the user interacts, via a network, with one or more resource sources. The method includes evaluating whether a resource directed to the client device is from a trusted resource source, displaying an icon on the client device that provides a visual indication of whether the resource is from a trusted resource source, and providing, in a control area of the client device, a data field for receiving input from the user to be sent to the resource source. The icon and data field together are a security application*); the security component comprising:

means for storing / storing, at the user terminal a plurality of resource locator patterns, each resource locator pattern matching one or more resource locators relating to Internet

resources known or believed to be associated with security risks (*Reno: [0022] a trust information source (such as trust authority 110) collects trust information from users, other trust authorities, independent monitoring, and the like. In some cases the information is evaluated, and false reports and the like are disregarded. The information may include known trusted sources, and known untrusted sources. The trusted list may include domain names, fully qualified domain names, Uniform Resource Identifiers ("URIs," such as URLs), and the like*);

means for receiving / receiving a resource locator from the browser application (*Reno: [0016] resources sources 106, 108 typically "host" web sites and send and receive resources (e.g., web pages) to users; [0025-0026] At block 204, the user sends a request for a resource. As those skilled in the art appreciate, this may involve typing a URL into an address window of a browser, selecting a stored "favorites" link, selecting a hyperlink in a web page, and the like....At block 214, the user device receives either or both of the resources from the trusted and untrusted sources*);

means for comparing / comparing the received resource locator to the stored resource locator patterns (*Reno: [0027] At block 216, the security application decides whether the resource is from a trusted source. In some embodiments, the application consults a trusted sites list, an untrusted sites list, a user-configured option, and/or the like to decide*); and

means for providing / providing a security alert if the received resource locator matches one of the stored resource locator patterns (*Reno: [0027-0028] If the source is not trusted, the process continues at block 218. At block 218, the application displays an untrusted site icon*).

Regarding claim 2, 35, Reno further taught a component according to claim 1 / a method according to claim 34, wherein the resource locators are character strings and the resource locator patterns are character patterns (*Reno: [0016, 0018]*).

Regarding claim 3, 36, Reno further taught a component according to claim 2 / a method according to claim 35, wherein the comparing means comprises means for testing the resource locator for the presence of one or more characters specified by a character pattern (*Reno: [0027] At block 216, the security application decides whether the resource is from a trusted source. In some embodiments, the application consults a trusted sites list, an untrusted sites list, a user-configured option, and/or the like to decide*).

Regarding claim 51, Reno taught a method of providing security information to a user accessing via the internet accounts for holding or managing money or other tokens of value (*Reno: [0006] a method of facilitating interaction between a user at a client device and a resource source. The client device includes a user interface through which the user interacts, via a network, with one or more resource sources. The method includes evaluating whether a resource directed to the client device is from a trusted resource source, displaying an icon on the client device that provides a visual indication of whether the resource is from a trusted resource source, and providing, in a control area of the client device, a data field for receiving input from the user to be sent to the resource source. The icon and data field together are a security application*), comprising:

storing domain names and or IP address information relating to trusted internet sites providing access to such accounts (*Reno: [0022] a trust information source (such as trust authority 110) collects trust information from users, other trust authorities, independent monitoring, and the like. In some cases the information is evaluated, and false reports and the like are disregarded. The information may include known trusted sources, and known untrusted sources. The trusted list may include domain names, fully qualified domain names, Uniform Resource Identifiers ("URIs," such as URLs), and the like*);

receiving a resource locator specifying an internet resource requested by the user (*Reno: [0016] resources sources 106, 108 typically "host" web sites and send and receive resources (e.g., web pages) to users; [0025-0026] At block 204, the user sends a request for a resource. As those skilled in the art appreciate, this may involve typing a URL into an address window of a browser, selecting a stored "favorites" link, selecting a hyperlink in a web page, and the like....At block 214, the user device receives either or both of the resources from the trusted and untrusted sources*);

determining whether the resource locator relates to a trusted Internet site by comparing a domain name or IP address associated with the resource locator to the stored domain names and/or IP address information (*Reno: [0027] At block 216, the security application decides whether the resource is from a trusted source. In some embodiments, the application consults a trusted sites list, an untrusted sites list, a user-configured option, and/or the like to decide*); and

outputting a corresponding indication to the user if it is determined that the resource locator does relate to a trusted internet site (*Reno [0005]*).

Regarding claim 53, Reno further taught a security information server adapted to carry out a method as claimed in Claim 34 (*Reno, [0016]*).

Regarding claim 54, Reno further taught a computer program or computer program product comprising a security component as claimed in claim 1 (*Reno, Abstract, fig. 1-3B*).

Regarding claim 55, Reno further taught a computer program or computer program product comprising software code adapted, when executed on a data processing apparatus, to perform a method as claimed in claim 34 (*Reno, Abstract, fig. 1-3B*).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4-5, 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reno in view of Bellinson et al. US 2004/0006621 hereinafter "Bellinson"

> Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Regarding claim 4, Reno taught a component according to claim 1, Reno was silent on adapted to process a pattern comprising one or more wildcards or placeholders. However this claim limitation is well-known as admitted by the applicant (*see spec, page 19-31, Examples of toolbars available for Microsoft Internet Explorer.TM. include the Alexa toolbar (developed by Alexa Internet) and the Google toolbar (provided by Google, Inc. As described above, the toolbar provides both local and remote checking of URLs requested by the user, In particular, the local checks involve detecting suspicious characters or character patterns which might indicate that the URL is associated with some kind of fraud attempt*) and also Bellinson, which addressed the same field of endeavor in controlling user access to a site taught adapted to process a pattern comprising one or more wildcards or placeholders (*Bellinson, [0048-49]*).

Therefore, it would have been obvious to one having ordinary skilled in the art at the time the applicant's invention was made to modify the invention of Reno with the teaching of Bellinson for the use of pattern comprising wildcards or placeholders because the use of

Bellinson could provide Reno (*Reno, fig. 3A, 3B*) the ability to include wildcards or placeholders for pattern processing to create "allowed" "Blocked list" to apply the allow or block designation to all web page at or below the specific domain level (*Bellinson, [0048]*).

Regarding claim 5, 37, Reno in view of Bellinson further taught a component according to claim1 / a method according to claim 34, further comprising means for receiving / receiving, at user terminal pattern update information; and means for updating the resource locator patterns stored by the storing means in response to the update information /(*Reno, [0022-23; 0018; see also Bellinson [0051-52]*).

Claims 6 -18, 38-50, 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reno in view of William et al. WO 01/98934 hereinafter "William"

Regarding claim 6, Reno taught a component according to Claim 1, and inherently taught further comprising means for transmitting a representation of the resource locator to a security information server, and means for receiving security information relating to the resource locator from the security information server (*Reno, [0016] The resource sources 106, 108 may be any computing device capable of network communication, although the resource sources 106,108 typically are web servers. Examples of resource sources include servers, workstations, personal computers, and the like. Thus, resources sources 106, 108 typically "host" web sites and send and receive resources (e.g., web pages) to users*). However, William who addressed the same field of endeavor in internet content filtering taught transmitting a representation of the resource locator to a security information server, and means for receiving security information relating to the resource locator from the security information server (*William, Abstract: An internet content filtering software comprises two components. One component runs on an Internet server and the other component runs locally on a user's computer system. The two components cooperate with one another to filter Internet*

content, with each component performing separate tasks. The Internet server component stores user profiles, a list and/or a table of permitted and prohibited Uniform Resource Locators (URLs), and receives redirected URL requests. Redirected URL requests are utilized, in conjunction with a user's profile, to determine whether access is granted or denied to the content associated with the URL).

Therefore, it would have been obvious to one having ordinary skilled in the art at the time the applicant's invention was made to modify the invention of Reno with the teaching of William for the use of transmitting/receiving security information to/from security information server because the use of William could provide Reno (*Reno, fig. 3A, 3B*) the ability to include security information server for consistent internet filtering when access to the internet is made from various computer systems (*William, [5:33-34]*).

Regarding claim 7, Reno in view of William further taught a component according to claim 6, wherein the representation comprises a check sum or hash code of at least part of the resource locator, further comprising means for generating the check sum or hash code (*Reno, [0031] [0013]*) .

Regarding claim 8, Reno in view of William further taught a component according to Claim 6 wherein the security information comprises a risk rating specifying an estimate of security risk associated with the resource locator (*Reno, [0028-0029]*).

Regarding claim 9, Reno in view of William further taught a component according to claim 6, wherein the security information comprises an indicator indicating whether the resource locator is associated with a trusted Internet location (*Reno, [0004] The one or more applications include a security application that includes at least one data field for receiving input from the user to be sent to a specific resource source and an icon that provides a visual indication of whether the specific source is a trusted resource source*).

Regarding claim 10, Reno in view of William further taught a component according to Claim 6, wherein the security information comprises IP registration information relating to an IP address with which the resource locator is associated (*Reno, [0016] resources sources 106, 108 typically "host" web sites and send and receive resources (e.g., web pages) to users. It is also to be understood that a particular resource source may host numerous web sites (i.e., resources), some of which may be trusted and some not, as will be explained. A web site /web page must have an IP address*),

Regarding claim 11, Reno in view of William further taught a component according to claim 6, further comprising means for displaying the security information (*Reno, [0028]*).

Regarding claim 12, Reno in view of William further taught a component according to claim 1, wherein the alerting means is adapted to prevent the Internet browser application from displaying the Internet resource specified by the resource locator (*Reno, [0020] the data field(s) are "grayed out," so that the user cannot enter the sensitive information. Thus, through a combination of operations, the security application attempts to prevent the user from divulging sensitive information to an untrusted source, See further [0030] users are conditioned to attempt to enter sensitive information into the tool bar, or other appropriate location, depending upon the embodiment of the security application (e.g., a dialog box in a standalone application, or the like)*).

Regarding claim 13, the combination of Reno and William further taught a component according to Claim 1 further comprising means for receiving an indication of a suspected security risk from a user of the internet browser application relating to an internet resource viewed by the user, and means for transmitting the indication to a security information server (*William, [7:31-8:40] : the server provides a centralized resource for site blocking functionality. The user computers, however, perform content filtering and update the database of prohibited URLs maintained at the server, based on the results of the local scanning performed during content filtering. The central*

server also stores user profile data, and downloads the latest updated version of a user's profile to the terminal computer each time that a particular user accesses the internet).

Therefore, it would have been obvious to one having ordinary skilled in the art at the time the applicant's invention was made to modify the invention of Reno with the teaching of William for the use of transmitting/receiving security information to/from security information server because the use of William could provide Reno (*Reno, fig. 3A, 3B*) the ability to include security information server for consistent internet filtering when access to the internet is made from various computer systems (*William, [5:33-34]*).

Regarding claim 14, Reno taught a security component (*Reno: [0005] The security application may include a plug-in to the web browser, The security application may be a tool bar, a dialog box, a popup window, a standalone application, and/or the like*) for use with an Internet browser application which displays Internet resources (*Reno: [0005] The one or more resource sources may be web sites, See also [0016]*) in response to resource locators specifying the internet resources (*Reno: [0006] a method of facilitating interaction between a user at a client device and a resource source. The client device includes a user interface through which the user interacts, via a network, with one or more resource sources. The method includes evaluating whether a resource directed to the client device is from a trusted resource source, displaying an icon on the client device that provides a visual indication of whether the resource is from a trusted resource source, and providing, in a control area of the client device, a data field for receiving input from the user to be sent to the resource source. The icon and data field together are a security application*); the security component comprising:

means for receiving a resource locator from the browser application (*Reno: [0016] resources sources 106, 108 typically "host" web sites and send and receive resources (e.g., web pages) to users; [0025-0026] At block 204, the user sends a request for a resource. As those skilled in the art*

appreciate, this may involve typing a URL into an address window of a browser, selecting a stored "favorites" link, selecting a hyperlink in a web page, and the like....At block 214, the user device receives either or both of the resources from the trusted and untrusted sources) ;

means for receiving IP registration information relating to the resource locator from the remote server (*Reno, [0016] resources sources 106, 108 typically "host" web sites and send and receive resources (e.g., web pages) to users. It is also to be understood that a particular resource source may host numerous web sites (i.e., resources), some of which may be trusted and some not, as will be explained. A web site /web page must have an IP address;* it is also noted that getting IP registration information using "whois" was well known in the art at the time the applicant's invention was made. An ordinary skill in the art can easily implement whois in his/her invention); and

means for displaying the IP registration information (*Reno, [0028]*).

Reno taught a component according to Claim 1, and inherently taught means for transmitting a representation of the resource locator to a remote server (*Reno, [0016] The resource sources 106, 108 may be any computing device capable of network communication, although the resource sources 106,108 typically are web servers. Examples of resource sources include servers, workstations, personal computers, and the like. Thus, resources sources 106, 108 typically "host" web sites and send and receive resources (e.g., web pages) to users*). However, William who addressed the same field of endeavor in internet content filtering taught transmitting a representation of the resource locator to a remote server (*William, Abstract: An internet content filtering software comprises two components. One component runs on an Internet server and the other component runs locally on a user's computer system. The two components cooperate with one another to filter Internet content, with each component performing separate tasks. The Internet server component stores user profiles, a list and/or a table of permitted and prohibited Uniform Resource Locators (URLs), and receives redirected URL requests.*

Redirected URL requests are utilized, in conjunction with a user's profile, to determine whether access is granted or denied to the content associated with the URL).

Therefore, it would have been obvious to one having ordinary skilled in the art at the time the applicant's invention was made to modify the invention of Reno with the teaching of William for the use of transmitting/receiving security information to/from security information server because the use of William could provide Reno (*Reno, fig. 3A, 3B*) the ability to include security information server for consistent internet filtering when access to the internet is made from various computer systems (*William, [5:33-34]*).

Regarding claim 15, Reno in view of William further taught a security component according to claim 14, comprising a user interface for user interaction with the security component, the user interface being adapted to be integrated into the user interface of the Internet browser application (*Reno: fig. 3A/3B, [0005] the user interface may include means for interacting with a source of information relating to whether resource sources are trusted resource sources. The user interface may be a web browser. The security application may include a plug-in to the web browser. The security application may be a tool bar, a dialog box, a popup window, a standalone application, and/or the like*).

Regarding claim 16, Reno in view of William further taught a security component according to Claim 15, wherein the user interface comprises a display area for displaying security information relating to the resource locator (*Reno: [0005]*).

Regarding claim 17, 52, Reno in view of William further taught a plug-in for an Internet browser application comprising a component as claimed in claim 1 / a component, plug-in or toolbar for an internet browser application adapted to carry out a method as claimed in claim 34 (*Reno: [0005] The security application may include a plug-in to the web browser*).

Regarding claim 18, Reno in view of William further taught a toolbar for an Internet browser application comprising a component as claimed in claim 1 (*Reno: fig. 3A/3B, [0005] The user interface may be a web browser. The security application may include a plug-in to the web browser. The security application may be a tool bar, a dialog box, a popup window, a standalone application, and/or the like*).

Regarding claim 38, the combination of Reno and William further taught a method according to claim 34, further comprising:

maintaining, at a security information server, a database of security information relating to Internet locations (*William: Abstract, The Internet server component stores user profiles, a list and/or a table of permitted and prohibited Uniform Resource Locators (URLs)*);

retrieving security information relating to the received resource locator from the database (*William, Abstract: Redirected URL requests are utilized, in conjunction with a user's profile, to determine whether access is granted or denied to the content associated with the URL*); and

displaying the security information at rile user terminal (*Reno, [0028]*).

Regarding claim 39, Reno in view of William further taught a method according to Claim 38, further comprising: storing, at the security information server, a plurality of resource locator patterns, each resource locator pattern matching one or more resource locators relating to internet resources known or believed to be associated with security risks (*Reno: [0022] a trust information source (such as trust authority 110) collects trust information from users, other trust authorities, independent monitoring, and the like. In some cases the information is evaluated, and false reports and the like are disregarded. The information may include known trusted sources, and known untrusted sources. The trusted list may include domain names, fully qualified domain names, Uniform Resource Identifiers ("URIs," such as URLs), and the like*), and transmitting the resource locator

patterns to the user terminal (*Reno: [0027-0028] If the source is not trusted, the process continues at block 218. At block 218, the application displays an untrusted site icon*).

Regarding claim 40, the combination of Reno and William further taught a method according to Claim 39, further comprising receiving an indication of a suspected security risk relating to a specified resource locator from a user terminal; and adding a resource locator pattern matching the specified resource locator to the plurality of resource locator patterns stored at the security information server (*William, 11:-15: Tasks performed by the server software include ; controlling actual access to web sites responsive to the redirected URL requests; recording access to web sites for data mining purposes ; storing a configuration for each individual user as well as other user information; scanning web sites for inclusion into allowed or prohibited lists*).

Regarding claim 41, the combination of Reno and William further taught a method according to Claim 39, further comprising:

transmitting pattern version information from the user terminal to the security information server identifying the version of the local copy of the resource locator patterns held at the user terminal, and transmitting pattern update information from the security information server to the user terminal in dependence on the version information to update the local copy of the resource locator patterns (*William, [8:36-38], The central server also stores user profile data, and downloads the latest updated version of a user's profile to the terminal computer each time that a particular user accesses the Internet. See [5:11-13] automated manner for keeping blocked site lists updated with new sites on the Internet; see [19:25-30] The client is then set to the enabled mode at step 630, and a check is performed at step 635 to determine whether there are new versions of updateable files for the client. The check at step 635 accesses a database 120 via an access control server 115, and downloads new files from database 120 if there are new files to download.*).

Regarding claim 42, Reno in view William further taught a method according to claim 38, comprising calculating, based on information stored in the security information database, a risk rating specifying an estimate of security risk associated with an internet resource or location represented by the received resource locator, and displaying the calculated risk rating at the user terminal (*Reno, [0028-0029]: the icon's appearance may change in any of a number of ways. For example, the icon may be a specific color, green for example, when a source is trusted, and red when a source is untrusted. The icon may be larger in one case and smaller in the other Many other examples are possible.... The trust level may be a number on a scale or a color from a spectrum. The trust level may be calculated based on any of a number of factors, some of which may be configured by the user...*).

Regarding claim 43, the combination of Reno and William further taught a method according to claim 38, further comprising storing information relating to suspected security vulnerabilities associated with an internet location in the database (*William: Abstract, The Internet server component stores user profiles, a list and/or a table of permitted and prohibited Uniform Resource Locators (URLs)*).

Regarding claim 44, the combination of Reno and William further taught a method according to claim 43, further comprising assessing an internet location to determine whether potential security vulnerabilities are associated with the location, and storing the outcome of the assessment in the database (*William, 11:1-5: the client handles the logon procedure; performs real time content filtering ; learns from content filtering and causes Uniform Resource Locators ("URLs") to be blocked to be stored in a remote database 120*).

Regarding claim 45, the combination of Reno and William further taught a method according to Claim 44, wherein the assessing step comprises identifying potential security vulnerabilities in dependence on one or more of: the operating system of a web server associated

with the location, the version of that operating system, the web server software used by the web server, and the version of that web server (*William, [8:36-45]: The central server also stores user profile data, and downloads the latest updated version of a user's profile to the terminal computer each time that a particular user accesses the Internet. The user's profile for site blocking and the URL database are uniformly maintained and implemented at the internet server, and the downloading of profiles to terminal computers at time of access provides a uniform application of each user's profile for content scanning and filtering across multiple access platforms, see also 19:14-29*).

Regarding claim 46, the combination of Reno and William further taught a method according to claim 38, further comprising storing registration information relating to a plurality of IP addresses in the database, and wherein the retrieving step comprises retrieving registration information relating to an IP address associated with the received resource locator (*Reno, [0016] resources sources 106, 108 typically "host" web sites and send and receive resources (e.g., web pages) to users. It is also to be understood that a particular resource source may host numerous web sites (i.e., resources), some of which may be trusted and some not, as will be explained. A web site /web page must have an IP address,* it is also noted that getting IP registration information using "whois" was well known in the art at the time the applicant's invention was made. An ordinary skill in the art can easily implement whois in his/her invention).

Regarding claim 47, the combination of Reno and William further taught a method according to Claim 38, further comprising storing information relating to trusted Internet locations in the database, and wherein the retrieving step comprises determining whether the received resource locator relates to a trusted Internet location (*William: Abstract, The Internet server component stores user profiles, a list and/or a table of permitted and prohibited Uniform Resource Locators (URLs)*; *Reno, [0004] The one or more applications include a security application that includes*

at least one data field for receiving input from the user to be sent to a specific resource source and an icon that provides a visual indication of whether the specific source is a trusted resource source).

Regarding claim 48, the combination of Reno and William further taught a method according to Claim 47, wherein the information comprises a list of trusted domain names (*William, Abstract*).

Regarding claim 49, the combination of Reno and William further taught a method according to Claim 47, wherein the information comprises a list of trusted IP addresses or IP address ranges (*William, abstract: The Internet server component stores user profiles, a list and/or a table of permitted and prohibited Uniform Resource Locators (URLs)*).

Regarding claim 50, the combination of Reno and William further taught a method according to claim 34**,** wherein the alerting step comprises preventing the Internet browser application from displaying the Internet resource specified by the resource locator. (*Reno: [0027-0028] If the source is not trusted, the process continues at block 218. At block 218, the application displays an untrusted site icon; see also [0030]*).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 19-23, 25-27 are rejected under 35 U.S.C. 102(b) as being anticipated by William et al. WO 01/98934 hereinafter "William"

> Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the

limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Regarding claim 19, William taught a security information server (*William: Abstract: An internet content filtering software comprises two components. One component runs on an Internet server and the other component runs locally on a user's computer system.*) comprising:

a database of security information relating to Internet locations (*William: Abstract, The Internet server component stores user profiles, a list and/or a table of permitted and prohibited Uniform Resource Locators (URLs)*) ;

means for receiving a security information request comprising a representation of a resource locator from a user terminal (*William, Abstract: receives redirected URL requests*) ;

means for retrieving security information relating to the resource locator from the database (*William, Abstract: Redirected URL requests are utilized, in conjunction with a user's profile, to determine whether access is granted or denied to the content associated with the URL*); and

means for transmitting the security information to the user terminal (*William, 6: 29-31: The transmitted URL is then logged in association with the user's identifier. If the user is not granted access to the URL then the user's computer system displays an appropriate message*).

Regarding claim 20, William further taught a security information server according to Claim 19, further comprising:

means for receiving security information relating to a specified resource locator from a user terminal; and means for updating the database in dependence on the security information received (*William, 7:32-8:02: The user computers, however, perform content filtering and update the database of prohibited URLs maintained at the server, based on the results of the local scanning*

performed during content filtering. Stated another way, each user's computer becomes a resource for reviewing internet content and updating the URL database).

Regarding 21, William further taught a security information server according to Claim 19, wherein the database is adapted to store a plurality of resource locator patterns, each resource locator pattern matching one or more resource locators relating to Internet resources known or believed to be associated with security risks (*William, 13:15-20: The server utilizes a list of prohibited URLs and a list of approved URLs, typically stored on database 120, Abstract, The Internet server component stores user profiles, a list and/or a table of permitted and prohibited Uniform Resource Locators (URLs)*).

Regarding claim 22, William further taught a security information server according to claim 21, further comprising means for receiving an indication of a suspected security risk relating to a specified resource locator from a user terminal; and means for adding a resource locator pattern matching the specified resource locator to the stored resource locator patterns (*William, 11:-15: Tasks performed by the server software include ; controlling actual access to web sites responsive to the redirected URL requests; recording access to web sites for data mining purposes ; storing a configuration for each individual user as well as other user information; scanning web sites for inclusion into allowed or prohibited lists*).

Regarding claim 23, William further taught a security information server according to further comprising means for receiving pattern version information from a user terminal specifying the version of a local copy of the resource locator patterns held at the user terminal, and means for transmitting pattern update information to the user terminal in dependence on the version information to update the local copy of the resource locator patterns (*William, [8:36-38], The central server also stores user profile data, and downloads the latest updated version of a user's*

profile to the terminal computer each time that a particular user accesses the Internet. See [5:11-13] automated manner for keeping blocked site lists updated with new sites on the Internet; see [19:25-30] The client is then set to the enabled mode at step 630, and a check is performed at step 635 to determine whether there are new versions of updateable files for the client. The check at step 635 accesses a database 120 via an access control server 115, and downloads new files from database 120 if there are new files to download.).

Regarding claim 25, William further taught a security information server according to claim 19, wherein the database is adapted to store information relating to suspected security vulnerabilities associated with an Internet location (*William: Abstract, The Internet server component stores user profiles, a list and/or a table of permitted and prohibited Uniform Resource Locators (URLs)*).

Regarding claim 26, William further taught a security information server according to Claim 25, further comprising means for assessing whether potential security vulnerabilities are associated with an Internet location (*William, Abstract: determine whether access is granted or denied to the content associated with the URL*).

Regarding claim 27, William further taught a security information server according to Claim 26, wherein the assessing means is adapted to identify potential security vulnerabilities in dependence on one or more of: the operating system of a web server associated with the location, the version of that operating system, the web server software used by the web server, and the version of that web server software (*William, [8:36-45]: The central server also stores user profile data, and downloads the latest updated version of a user's profile to the terminal computer each time that a particular user accesses the Internet. The user's profile for site blocking and the URL database are uniformly maintained and implemented at the internet server, and the downloading of profiles to terminal*

computers at time of access provides a uniform application of each user's profile for content scanning and filtering across multiple access platforms, see also 19:14-29).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 24, 28-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over William et al. WO 01/98934 hereinafter "William" in view of Reno

> Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Regarding claim 24, William taught a security information server according to *7* claim 19, William was silent on, further comprising means for calculating a risk rating specifying an estimate of security risk associated with an internet resource or location referred to by the resource locator, and means for transmitting the calculated risk rating to the user terminal.

However the analogous art Reno, which addressed the same field of endeavor in browser interface security, taught calculating a risk rating specifying an estimate of security risk associated with an internet resource or location referred to by the resource locator, and means for transmitting the calculated risk rating to the user terminal (*Reno, [0028-0029]: the icon's appearance may change in any of a number of ways. For example, the icon may be a specific color, green for example, when a source is trusted, and red when a source is untrusted. The icon may be larger in one*

case and smaller in the other Many other examples are possible.... The trust level may be a number on a scale or a color from a spectrum. The trust level may be calculated based on any of a number of factors, some of which may be configured by the user...).

Therefore it would have been obvious to one having ordinary skilled in the art at the time the applicant's invention was made to modify the invention of William with the teaching of Reno for the use of calculating risk level and transmitting rating to the user terminal (*Reno, [0028-0029]*) because the use of Reno could provide William (*William, fig. 16, 17*) the ability to include calculating risk rating and transmitting to the user terminal to provide visual indication of a level of trust of the resource source (*Reno, [0007]*).

Regarding claim 28, the combination of William and Reno further taught a security information server according to claim 19, wherein the database is adapted to store registration information relating to a plurality of IP addresses, and wherein the retrieving means is adapted to retrieve registration information relating to an IP address associated with the received resource locator representation (*Reno, [0016] resources sources 106, 108 typically "host" web sites and send and receive resources (e.g., web pages) to users. It is also to be understood that a particular resource source may host numerous web sites (i.e., resources), some of which may be trusted and some not, as will be explained. A web site /web page must have an IP address,* it is also noted that getting IP registration information using "whois" was well known in the art at the time the applicant's invention was made. An ordinary skill in the art can easily implement whois in his/her invention).

Regarding claim 29, the combination of William and Reno further taught a security information server according to claim 28, wherein the registration information comprises information relating to the organization or person to whom the IP address is registered (*Reno, [0016, 0028]*).

Regarding claim 30, the combination of William and Reno further taught a security information server according to claim 19, wherein the database is adapted to store information relating to trusted Internet locations, the security information server further comprising means for determining whether the received resource locator representation relates to a trusted internet location, the transmitted security information comprising an indicator indicating whether the received resource locator representation relates to a trusted internet location (*William: Abstract, The Internet server component stores user profiles, a list and/or a table of permitted and prohibited Uniform Resource Locators (URLs)*; *Reno, [0004] The one or more applications include a security application that includes at least one data field for receiving input from the user to be sent to a specific resource source and an icon that provides a visual indication of whether the specific source is a trusted resource source*).

Regarding claim 31, the combination of William and Reno further taught a security information server according to Claim 30, wherein the information comprises a list of trusted domain names (*William, Abstract*).

Regarding claim 32, (Currently Amended) the combination of William and Reno further taught a security information server according to claim 30**,** wherein the information comprises a list of trusted IP addresses or IP address ranges (*William, abstract: The Internet server component stores user profiles, a list and/or a table of permitted and prohibited Uniform Resource Locators (URLs)*).

Regarding claim 33, the combination of William and Reno further taught a security information system comprising a security information server as claimed in claim 19 and a plurality of user terminals each comprising a security component, wherein the security component comprises:

means for storing a plurality of resource locator patterns, each resource locator pattern matching one or more resource locators relating to internet resources known or believed to be associated with security risks (*Reno: [0022] a trust information source (such as trust authority 110) collects trust information from users, other trust authorities, independent monitoring, and the like. In some cases the information is evaluated, and false reports and the like are disregarded. The information may include known trusted sources, and known untrusted sources. The trusted list may include domain names, fully qualified domain names, Uniform Resource Identifiers ("URIs," such as URLs), and the like*);

means for receiving a resource locator from the browser application (*Reno: [0016] resources sources 106, 108 typically "host" web sites and send and receive resources (e.g., web pages) to users; [0025-0026] At block 204, the user sends a request for a resource. As those skilled in the art appreciate, this may involve typing a URL into an address window of a browser, selecting a stored "favorites" link, selecting a hyperlink in a web page, and the like....At block 214, the user device receives either or both of the resources from the trusted and untrusted sources*);

means for comparing the received resource locator to the stored resource locator patterns (*William, [12:3-10]; Reno: [0027] At block 216, the security application decides whether the resource is from a trusted source. In some embodiments, the application consults a trusted sites list, an untrusted sites list, a user-configured option, and/or the like to decide*); and

means for providing a security alert if the received resource locator matches one of the stored resource locator patterns (*Reno: [0027-0028] If the source is not trusted, the process continues at block 218. At block 218, the application displays an untrusted site icon*).

Therefore it would have been obvious to one having ordinary skilled in the art at the time the applicant's invention was made to modify the invention of William with the teaching of Reno

because the use of Reno could provide William (*William, fig. 16, 17*) the ability to provide visual indication of a level of trust of the resource source (*Reno, [0007]*).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MOHAMMAD L. RAHMAN whose telephone number is (571)270-7471. The examiner can normally be reached on Monday-Friday (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. L. R./
Examiner, Art Unit 2438

/Taghi T. Arani/

Supervisory Patent Examiner, Art Unit 2438